Amendments to the Claims:
This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A consumable authentication protocol for validating the authenticity of an untrusted authentication chip, the protocol includes the steps of:

generating an original random number in a trusted authentication chip; ~~and~~

applying, in the trusted authentication chip, an asymmetric encrypt function to the original random number using a first key from the trusted authentication chip to produce a first encrypted outcome;

passing the first encrypted outcome to the untrusted authentication chip;

decrypting, in the untrusted authentication chip, the first encrypted outcome with an asymmetric decrypt function using a second secret key from the untrusted authentication chip to produce a second decrypted outcome~~, in the untrusted chip~~;

applying, in the untrusted authentication chip, ~~the~~ an asymmetric encrypt function to the second decrypted outcome together with an original data message read from the untrusted authentication chip using the second secret key to produce a third encrypted outcome~~, in the untrusted chip~~;

passing the ~~receiving the~~ third encrypted outcome together with the original data message ~~together with the data message~~ to the trusted authentication chip;

decrypting, in the trusted authentication chip, the third encrypted outcome with an asymmetric decrypt function using the first key to produce ~~and comparing the~~ a decrypted random number and a decrypted data message;

comparing the decrypted random number and the decrypted data message with the ~~generated~~ original random number and the received original data message, without knowledge of the second secret key; and,

in the event of a match, considering the untrusted chip and the data message to be valid;

otherwise considering the untrusted chip and the data message to be invalid.

2. (Original) A consumable authentication protocol according to claim 1, for validating the authenticity of an untrusted authentication chip, as well as ensuring that the authentication chip, lasts only as long as the consumable including the further steps of writing new data to the untrusted chip, performing the steps of claim 1, and in the event the untrusted chip is found to be authentic and the new data is the same as the data message read from the untrusted chip, then the write is validated.

3. (Original) A consumable authentication protocol according to claim 1, where the first key is a public key.

4. (Original) A consumable authentication protocol according to claim 1, where encryption outside the untrusted chip is implemented in software.

5. (Original) A consumable authentication protocol according to claim 4, where the random number generation, encryption, passing, and final decrypting and comparing steps take place in an external system.

6. (Original) A consumable authentication protocol according to claim 5, where the external system is in a printer or other device in which consumables such as ink cartridges are mounted.

7. (Original) A consumable authentication protocol according to claim 6, where the untrusted chip is in the consumable.

8. (Original) A consumable authentication protocol according to claim 1, where the encryption outside the untrusted chip is implemented in a second authentication chip, and an external system intermediates between the two chips.

9. (Original) A consumable authentication protocol according to claim 8, where the second authentication chip and system are in a printer or other device in which consumables are mounted.

10. (Original) A consumable authentication protocol according to claim 9, where the untrusted chip is in the consumable.

11. (Original) A consumable authentication protocol according to claim 1, where the secret key is held only by the untrusted chip.

12. (Original) A consumable authentication protocol according to claim 1, where the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every successful authentication so that the next random number will be produced from a different seed.

13. (Original) A consumable authentication protocol according to claim 1, where the data message is a memory vector of the authentication chip, a part is different for each chip, and parts of it are constant (read only) for each consumable, or decrement only so that it can be completely downcounted only once for each consumable.

14. (Currently amended) A consumable authentication system for validating the authenticity of an untrusted authentication chip, where the system comprises:

a random number generator to generate an original random number in a trusted authentication chip;

an asymmetric encryptor to encrypt the generated original random numbers with an asymmetric encryption function to produce a first encrypted outcome ~~and~~ using a first key for the encryptor;

an untrusted authentication chip, the untrusted authentication chip including a read function which operates to decrypt the first encrypted outcome using a second secret key and produce a second decrypted outcome, then applies the symmetric encrypt function to the second decrypted outcome together with an original data message read using the second secret key to produce a third encrypted outcome, also returning the third encrypted outcome together

with ~~a clear~~ the original data message; and,

a test function, the test function operating to decrypt the third encrypted outcome using the first key to produce a decrypted random number and a decrypted data message, and compare the decrypted ~~second outcome~~ random number and decrypted data message with the generated original random number and the ~~clear~~ received original data message, without knowledge of the second secret key;

whereby, in the event of a match the test function returns a value indicating validity, otherwise the test function returns a value indicating invalidity.

15. (Original) A consumable authentication system according to claim 14, where new data written to the untrusted chip is considered valid in the event the untrusted chip is found to be authentic and the new data is the same as the data message read from the untrusted chip.

16. (Original) A consumable authentication system according to claim 14, where the first key is a public key.

17. (Original) A consumable authentication system according to claim 14, where encryption outside the untrusted chip is implemented in software.

18. (Original) A consumable authentication system according to claim 17, where the random number generation, encryption, passing, and final decrypting and comparing steps take place in an external system.

19. (Original) A consumable authentication system according to claim 18, where the external system is in a printer or other device in which consumables such as ink cartridges are mounted.

20. (Original) A consumable authentication system according to claim 19, where the untrusted chip is in the consumable.

21. (Original) A consumable authentication system according to claim 14, where the encryption outside the untrusted chip is implemented in a second authentication chip, and an external system intermediates between the two chips.

22. (Original) A consumable authentication system according to claim 21, where the second authentication chip and system are in a printer or other device in which consumables are mounted.

23. (Original) A consumable authentication system according to claim 22, where the untrusted chip is in the consumable.

24. (Original) A consumable authentication system according to claim 14, where the secret key is held only by the untrusted chip.

25. (Original) A consumable authentication system according to claim 14, where the random number generator of the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every successful authentication so that the next random number will be produced from a new seed.

26. (Original) A consumable authentication system according to claim 25 where for a group of authentication chips, the initial seed for each chip is different from that of the others in the group so that the first random number produced by each chip in the group will be different.

27. (Original) A consumable authentication system according to claim 14, where the data message is a memory vector of the authentication chip, a part is different for each chip, and parts of it are constant (read only) for each consumable, or decrement only so that it can be completely downcounted only once for each consumable.